

Agenda

- MITRE What is it and how to leverage it
- Modern Day Threats and "Pain"
- MITRE Threat-Informed Defense
- Summary & Resources



MITRE

Not-for-profit company to provide engineering and technical guidance for the federal government.

Created an advanced airdefense framework for the Air Force.
out of MIT laboratories
Est. 1958



Invented the concept of a CVE (Common Vulnerability & Exposures)

Bridging the gap between Gov & Industry

Sponsored by CISA (DHS)
Est. 1999



A Real-World TTP Knowledgebase

Cyber adversary Model describing Tactics, Techniques and Procedures

The foundation of Threat-Informed Defense

Est. 2013-15



A Foundation for Public Good

ATT&CK* Evaluations

2019 – Gothic Panda 2020 – Cozy Bear 2021 - Carbanak + FIN7 2022 – Wizard Spider + Sandworm



Leveraging MITRE ATT&CK Framework

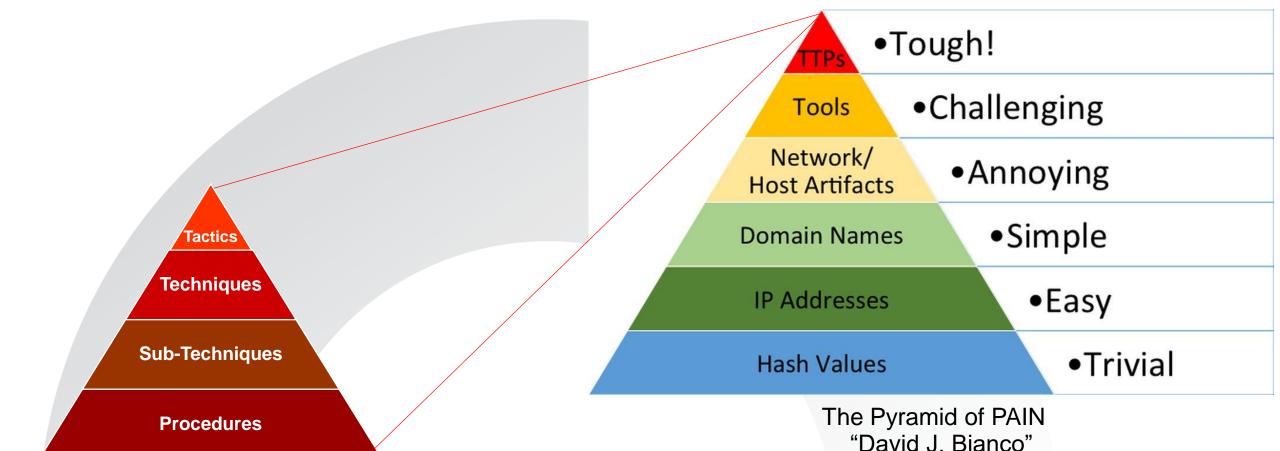
- Best measurement of capability
- Historical Visibility & Analytics
- Protections and detection capability
- Identify gap areas with current tooling

 Quickly understand Why & How the Attack Happened

• Faster Mean Time to Detect (MTTD)

• Improves Mean Time to Respond (MTTR)





"Threat-informed defense" applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks. It's a community-based approach to a worldwide challenge."





MITRE ATT&CK Matrix

,													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Asidore Stocarding (c)	Acquire Infrastructure (7)	Drive-by Compromise	Recording a	Account Manipulation (5)	Alexand Managillari Bertingi	Abuse Elevation Control Mechanism (4)	Adversary-in- the-Middle (3)	Removate Whiteerstory (4)	Exploitation of Remote	Aubsersory-in- the Whitele gal	Application Layer II	Autométeó Beiltíreiden (1)	Account Access Removal
Gentoer Viction Glassi Information ₆₀	Compromise	Exploit Public-	pugaskrayar Mil	BITS Jobs	(A) melcovise(A)	Assess Telson	Brute Force (4)	Application Window Discovery	Services	Azehtza	Protocol (4)	Data Transfer	Data Destruction
Centrer Victim Islamity	Associate 40	Facing Application	Container Administration	Boot or Logon	Assess Tallian Manipulation (4)	Manipulation (4)	@restenitete	Browser Bookmark	Internal Spearphishing	Collocated III Vede (e)	Communication Through	Size Limits	Data Encrypted for
hrömmstörr ₆₀	Compromise Infrastructure (7)	External	Command Deales Containes	Autostart II Execution (14)	Boot or Logon	BITS Jobs	Trum Passement II Steres _{pp}	Discovery	Lateral Tool	Audio Capture	Removable Media	Exfiltration Over	Impact
Gather Victim Network	Develop Conshilition	Remote Services	Deploy Container	Sael er Legen Initialization	Autostart Execution (14)	Build Image on Host	Exploitation for Credential	Cloud Infrastructure Discovery	Transfer Peopels	Automated Collection	Point II	Alternative Protocol (3)	Moin Manipulation po
Information (6)	Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Sheripiki (a)	Boot or Logon Initialization	Debugger Evasion Deobfuscate/Decode	Access	Cloud Service Dashboard	Sandes Sassion	Browser	Encesting pa	Exfiltration Over C2	Defacement (2)
Internation 66	Assertates ₍₈₀₎	Phistolog pp	Inter-Process Communication (3)	Browser Extensions	Scripts (5)	Files or Information	Forced Authentication	Cloud Service	Hijmelskryt _{gap}	Session Hijacking	Meliceciten (4)	Channel	Blaic Whyse ₄₉₀
Phishing for Information (3)	Whosin Capabilities _{Ma}	Replication	Native API	Compromise	Create or Modify System	Deploy Container	Forga Walt	Discovery	Remote Services (6)	Clipboard Data	Dynamic Resolution (3)	Esilitation Rear Wher	Endpoint Denial of Service (4)
Secreta Glorecal		Through Removable	Scheduled	Client Software Binary	Process (4)	Direct Volume Access	Greekanitaka 😝	Cloud Storage Object Discovery	Replication	Data from	Encrypted	Medium (1)	Firmware
Энцине _{ра}	Siege Capabilhies ₍₄₎	Media	Task/Job (5)	Orania	Bernala Palley Nicelifeature pa	Bernstn Pelicy ModPacker 46	trout Gapiura _{pa}	Container and	Through Removable	Cloud Storage	Channel (2)	Exfiltration	Corruption
Secula Open Technical II		Supply Chain Compromise est	Serverless Execution	Assessivi.	Escape to Host	Reconsiden description of	Research	Resource Discovery	Media	Data from Configuration	Fallback Channels	Over Physical II Medium (1)	Inhibit System Recovery
Defetosoce (d)		Trusted	Shared Modules	Oresic or Jobel by Oyenern III	Event Triggered	Exploitation for	Author/Aceilen III Process py	Debugger Evasion	Software Deployment	Repository (2)	Ingress Tool	Exfiltration	Heriaretk Benfel ef
Sourch Open Websites/Normains an		Relationship	Software	Present 68	Execution (16)	Defense Evasion	Multi-Factor	Domain Trust Discovery	Tools	Nation from Information II	Transfer	Over Web Service (2)	parotes M
Search Victim-Owned		Valid Amountitic (4)	Deployment Tools	Event linggered Reconsider (sep	Exploitation for Privilege	Missing Permissions II	Authentication Interception	File and Directory	Taint Shared Content	Napasaharisa ₍₄₎	Multi-Stage Channels	Scheduled	Resource Hijacking
Websites			System Services (2)	External Remote Services	Escalation Ntask	Mids Arthreis per	Multi-Factor Authentication	Discovery Group Policy Discovery	Use Alternais Authoritiesikan III	Data from Local System	Non-Application Layer Protocol	Transfer Transfer Data	Service Stop
			Windows	11 justs	Execution II	Hijisak Essaudian	Request Generation	Network Service	Majajaj (4	Data from Network	Non-Standard	to Cloud Account	System Shutdown/Reboot
			Management Instrumentation	Boseniden II Flator _{17,00}	Prevene	Plant (va)	Network	Discovery		Shared Drive	Port	ACCOUNT	Shutuowny Neboot
			mon amondanon	Implant Internal	trijookken (12)	Iroquatr Mariarnease (sp.	Sniffing	Network Share Discovery		Data from Removable	Protocol Tunneling		
				Image	Seheduled Tedo/Jole ed	Indherier Pernevel pp III	Os Oradaridal Dumping eg	Network Sniffing		Media	Possy (a)		
				Modify Authentication	Valid	Indirect Command Execution	Steal	Password Policy		Retin Stoyed pg	Remote Access		
				Process (7)	Assouris (4	Masquareding (6)	Application Access Token	Discovery		Erne)i Calisatian ₍₄₀	Software		
				Office Application		Modify Author/Deplem	Steal or Forge	Peripheral Device Discovery		hypoth	Warine Rightshing 🙀 "		
				Startup (6)		Process (r)	Authentication Certificates	Parmissien Encys		Server Conture	Web Service (3)		
				Pro-WE Seel ph		Modify Cloud Compute Infrastructure (4)	Sheef or Penge Resiscons	Process Discovery		Screen Capture Video Capture			
				Teak/Jule _(c)		Modify Registry	Thekeis _{(Q}	Query Registry		video capture			
				Server Software Component (5)		Medify System Imaga pa	Steal Web Session	Remote System					
				Traffic		Network Boundary	Cookie	Discovery					



Summary

- Threat-Informed Defense
 - Optimize Cybersecurity programs (People, Process, and Technology)
 - Continuous validation of security controls
 - Evolve from reactive to proactive (CTI+ATT&CK)
 - Focus on threats that matter most
 - Visibility / Effectiveness

Resources

Information

- https://attack.mitre.org/
- medium.com/mitre-attack
- twitter.com/MITREattack
- linkedin.com/showcase/mitre-att&ck
- https://www.attackiq.com/threat-informeddefense/

Training

https://attack.mitre.org/resources/training/

Mitigations

https://attack.mitre.org/mitigations/enterprise/

Prioritize

 https://top-attack-techniques.mitreengenuity.org/calculator



Thank You

°SHI

Where you have the ability to provide funding specific to cyber defenses, we recommend making that dependent upon implementation and adherence to a Threat-Informed Defense strategy/program.

Relative to commercial entities, you may have to rely upon applicable regulatory requirements (e.g. PCI, SOX, cyber liability insurance requirements).

